Appendix E Trusted Facility Manual (TFM) Template

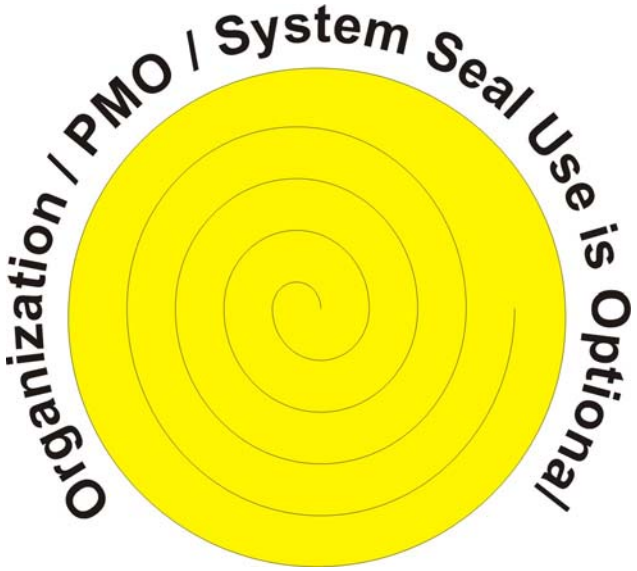
The purpose of a TFM is to document the necessary information to operate the system in a secure and effective manner. The requirement for a TFM is called out in DCID 6/3, which states:

> [Doc2] Documentation shall include guide(s) or manual(s) for the system's privileged users. The manual(s) shall at a minimum provide information on (1) configuring, installing, and operating the system; (2) making optimum use of the system's security features; and (3) identifying known security vulnerabilities regarding the configuration and use of administrative functions. The documentation shall be updated as new vulnerabilities are identified.

The TFM is not meant for general users of the system, but for use by those personnel designated as having specific security-related responsibilities. It provides information about the environment, roles, and responsibilities that guide security administrators and others with security responsibilities in the use of the security features provided by the IS. The TFM documents the configuration guidance used, operational requirements, security environment, hardware and software configurations and interfaces, and all security procedures, measures, and contingency plans for an IS. It also identifies know security vulnerabilities and any risk mitigation approaches employed.

A TFM should be produced by the PM/PMO during the development of an IS, and updated during any major change to the system. The TFM should also be reviewed and updated as necessary by site personnel upon delivery of a new or updated IS to reflect local system roles and responsibilities and local requirements. However, these local updates cannot be used to negate national policy or circumvent security features of the system as properly configured.
While some elements of the TFM cannot be completed by the PM/PMO during system development, it is not necessary for site personnel to complete portions of the TFM that are already documented elsewhere. Some of the information needed for the TFM may exist in documents such as in the site's security policy, site security concept of operations, or site configuration management/configuration control board policy. A reference to the appropriate site document and location of the applicable information (such as paragraph or section number) is sufficient in these cases.

This TFM template may be used as a guide for creating needed documentation needed to configure and maintain the security posture of a system.



Trusted Facility Manual
for the
[Name of System or Intelligence Mission Application]
at the
[Site Location]

Version [n.n]

[date]

[TSABI Number: nnnnnn (only if applicable)]

Prepared for:
[Program Office]

Prepared By:
[Preparer]

1 INTRODUCTION

1.1 Introduction to the [Enter the System Name Here] TFM

1.1.1 Purpose of the manual

This manual is intended to:

- Guide the secure configuration and installation of the system
- Guide the operation of the system in a secure manner
- Enable administrative personnel to make effective use of the system's privileges and protection mechanisms
- Issue warnings about possible misuse of administrative authority

1.1.2 Recommended use of the manual

This manual should be used to:

- Review skills and systems background necessary for security and system administrator personnel
- Suggest additional manuals, reference material, and standards, needed by security and system administrator personnel

1.2 Audience

This document is intended only for privileged users such as system/network administrators, ISSMs, ISSOs, etc.

1.3 Scope

Specify the limitations of security scope and guidelines for the security administrator to operate the system in a secure and effective manner. Also provide information about the environment, roles, and responsibilities that guide security administrator use of the security features and detailed system security features and procedures information for privileged users.

Enter Narrative Here

1.4 Product Trademark Registration

List the appropriate trademark notations; i.e., "Microsoft (MS) Windows New Technology (Windows NT®) operating system and other Microsoft™ products referenced herein are registered trademarks of Microsoft Corporation in the United States and other countries."

Enter Narrative Here

1.5 References

Provide a listing of directives, manuals, and other documents used as reference material. Include any security configuration guides used in the installation and secure configuration of the system.

Enter Narrative Here

2 SYSTEM SECURITY OVERVIEW

2.1 System Environment

Describe the organization(s) that the system supports and their location. Describe any security-specific components of the system architecture and the functions performed in addition to a high-level overall system architecture. Describe any network connections/interfaces. Document the classification of the data processed, the clearance level of the system's users, the Levels-of-Concern for Integrity and Availability and the Protection Level of the system. List the primary internal and external threats to the system and the countermeasures employed to mitigate them.

Enter Narrative Here

2.2 System and Security Management Roles and Responsibilities

At a minimum, define the roles and responsibilities with respect to the secure operation of the system for the following individuals: Information System Security Manager, Information System Security Officer, Network Security Manager, Network Security Officer, System Administrator, Computer Operators, Privileged User, Non-Privileged User.

Enter Narrative Here

2.3 System User Access Policy

This section describes each category of user and their access to system data and resources. The following is provided as a guide to help record the necessary information, but may be reformatted to suite the IS being described.

User Access Controls

Discuss all system user access controls (e.g., log-on ID, authenticators, file protections).

Enter Narrative Here

2.3.2. Assignment and Control of Authenticators

Discuss procedures for assignment and control of authenticators.

Enter Narrative Here

If Passwords are used to control access, complete section 2.3.3 through 2.3.8.

2.3.3. IS User Access

Check all boxes that apply to the passwords assigned to the IS users.

☐ All users have their own unique userid and unique password.

☐ Some users share a userid and password. (Explain below)

☐ **Some users share a password. (Explain below)**

2.3.4. Privileged User Access

Select only one level of access.

The privileged users have a unique userid and unique password at the:

☐ user level of access.

☐ superuser level of access.

2.3.5 Password Changes

Select one box only.

☐ Passwords are **NOT** changed.

☐ Users can change their passwords but are not forced to change their passwords on any timely basis, i.e., passwords are changed whenever the user feels it necessary to change his/her password.

☐ Users are forced to change their passwords every . . . *(Check all that apply)*

☐ Month ☐ 6 months ☐ Year ☐ **NEVER** ☐ After Initial Login

☐ Other (Specify)

2.3.6. Password Generation

Select all boxes that apply to the passwords.

☐ Passwords are generated by the user

☐ Users are encouraged by the ISSO or System Administrator to use "strong[1]" passwords whenever possible

☐ System software forces users to create "strong[1]" passwords

Please provide software or application that checks passwords:

Enter name of software/application here

☐ Passwords are generated by an IS

☐ Passwords are provided by an access control manager

Please provide office name:Enter Office Name Here

[1] A "strong" password is a password that contains a combination of alphanumeric characters to include multi-case and special characters, such as @, $, %, ^, &, etc.

2.3.7. Number of Allowed Login Attempts

Select one box only.

If a user enters the wrong userid or password:

☐ A time-out interval is enforced.

☐ **NOTHING** happens. The user can try to logon as many times as he or she wishes.

☐ Maximum number of attempts Enter # of Attempts Here

2.3.8. Account Lockout

Check all that apply

If a user's account is locked out due to excessive invalid logon attempts, who is authorized to reinstate the user's account?

☐ System Administrator
☐ ISSO
☐ Superuser
☐ Account Owner
☐ System automatically reinstates the account after a specified time period
☐ Other:(Specify)

2.4. User Groups and Access Rights

2.4.1. User Groups

Check all boxes that apply to the procedures followed to assign access rights to users and administrators.

☐	Users and administrators are **NOT** assigned to groups; all userids are at the same level.
☐	All groups have the same privileges/access rights; users have the same access rights as administrator.
☐	All administrators are assigned to a superuser group; the superuser group is different than the group(s) for users.
☐	All users are assigned to the same group. This group has fewer privileges/access rights than the privileged user group.
☐	Users are assigned to different groups depending on need-to-know and work assignments.
☐	User groups have different privileges/access rights depending on need-to-know and work assignments.
☐	Other: Specify

2.4.2. System Files

Select ONE box, only.

☐	Users **CANNOT** change the configuration and/or content of system files.
☐	Users can change the configuration and/or content of system files.

2.4.3. System Access Rights

Select ONE box, only.

☐	Users **CANNOT** set the system access rights of other users.
☐	Users can set the system access rights of other users.

2.4.4. Audit Log Access

Select all boxes that apply.

☐	Users **CANNOT** view, change, or delete the audit log.
☐	Users can view the audit log.
☐	Users can change or delete the audit log.

2.4.5. Privileged Users

Identify the number of privileged users and the criteria used to determine privileged access.

Enter Narrative Here

2.4.6. DAC/MAC

If DAC or MAC is required, discuss those mechanisms that implement the DAC and MAC controls.

Enter Narrative Here

3 SECURITY RELATED FEATURES AND PROCEDURES

Describe the security features of the system and detailed information about the who, what, when, where, why and how of each feature with respect to mitigating risk to the system. Describe the security operating procedures for the system with respect to users, roles, and responsibilities. Topics to be addressed may include:

- System startup and shutdown procedures and order (include servers, workstations, and other components, as applicable)
- Audit event definition and management
- Event log definition and management
- Audit reduction, review, and analysis
- Audit log archive and restore procedures
- Time synchronization
- Operating system updates
- Application updates
- Removable media handling procedures
- Anti-virus tasks
- Account management
- System and network management
- System security policy maintenance
- User groups and roles management
- Access Control List management

The following set of instructions may be used to begin recording the necessary information. All security-related topics and procedures should be included.

3.1 Protection of the Security Support Structure.

Discuss the protections provided to the Security Support Structure.

Enter Narrative Here

3.2 Security Features and Assurances.

3.2.1. Incident Reporting

Discuss procedures for incident reporting.

Enter Narrative Here

3.2.2. Remote Access

Discuss remote access and operations requiring specific approval by the Certifying Organization.

Enter Narrative Here

3.2.3 Change Control

Describe the procedures to ensure that changes to the system are coordinated with the ISSO before being implemented.

Enter Narrative Here

3.2.4 Configuration Management

Describe the configuration management program.

Enter Narrative Here

3.2.5 Security Features

Discuss any security features unique to the system.

Enter Narrative Here

3.2.6 System Startup

Discuss the procedures for system startup.

Enter Narrative Here

3.2.7 System Shutdown

Discuss the procedures for system shutdown.

Enter Narrative Here

3.3 Auditing

3.3.1 User-level Auditing

Discuss the auditing procedures used to monitor user access and operation of the system and the information that is to be recorded in the audit trail. State whether audit trails of user access are manual or automatic.

Enter Narrative Here

3.3.2 Audited Information

Check the boxes corresponding to the information provided for the audited events.

☐ Userid	☐ Type of event or action	☐ Resources
☐ Time	☐ Terminal or workstation id	☐ System location
☐ Date	☐ Success or failure of the event	☐ Entity that initiated transaction

3.3.3 Audited Activities

Check the box corresponding to the types of activities audited. Windows NT specific audit activities can be selected in a specific box below.

EVENT DESCRIPTION	Do you audit SUCCESS	Do you audit FAILURE	EVENT DESCRIPTION	SUCCESS	FAILURE
Logins	☐	☐	Logoffs	☐	☐
Printing	☐	☐	Copying data to removable media	☐	☐
Use of Superuser or root privileges	☐	☐	Read a file or directory	☐	☐
Creation of a file or data element(s)	☐	☐	Deletion of a file or data element(s)	☐	☐
Attempts to change data	☐	☐	Use of applications	☐	☐
Security relevant objects and incidents	☐	☐	Console	☐	☐

☐ The audit log is archived on magnetic media and maintained for a time period.

Enter the time period for on-line storage: Enter time period for storage here.

☐ days ☐ weeks ☐ months ☐ years

3.3.4 Audit Review

Identify the individual responsible for ensuring the review of audit trails and how often the reviews are performed.

Enter Narrative Here

3.3.5 Audit Handling

Describe the procedures for handling discrepancies found during audit trail reviews.

Enter Narrative Here

Marking and Labeling

3.4.1 Hardware

Describe how the system hardware will be labeled to identify its classification level, compartments, and handling controls.

Enter Narrative Here

3.4.2 Storage Media

Describe how the data storage media will be labeled to identify the classification level, compartments, handling controls, and information contents.

Enter Narrative Here

3.4.3 Hardcopy Output

Discuss procedures for marking and controlling system printouts.

Enter Narrative Here

3.5 Sanitization and Destruction

3.5.1 Hardware

Describe the procedures and methods used to sanitize hardware (volatile or nonvolatile components). If applicable, describe the procedures for declassification.

Enter Narrative Here

3.5.2 Software

Describe the procedures or methods used to clear, sanitize, and destroy the data storage media. If applicable, describe the procedures for declassification.

Enter Narrative Here

3.6 Software Security Procedures

3.6.1 Procurement

Describe the procedures for procuring and introducing system software.

Enter Narrative Here

3.6.2 Impact Evaluation

Describe the procedures for evaluating system software for security impacts.

Enter Narrative Here

3.6.3 Virus and Malicious Code Protection

Describe procedures for protecting software from computer viruses and malicious code and for reporting and responding to incidents.

Enter Narrative Here

3.6.4 Maintenance

Indicate whether a separate version of the operating system software will be used for maintenance.

Enter Narrative Here

3.7 Media Movement

3.7.1 Into and Out of Secure Facility

Describe the procedures or receipting methods for moving data storage media into and out of the secure facility.

Enter Narrative Here

3.7.2 Copy/Review/Release

Describe the procedures for copying, reviewing, and releasing information on data storage media.

Enter Narrative Here

3.8 Hardware control

3.8.1 System Transport

Describe the procedures or receipting methods used to release and transport the system hardware from the secure facility.

Enter Narrative Here

3.8.2 System Relocation

Describe the procedures or receipting methods for temporarily or permanently relocating the system hardware within the secure facility.

Enter Narrative Here

3.8.3 Control/Operation/Maintenance

Describe the procedures for the secure control, operation, and maintenance of the hardware. If they have been authorized, describe the procedures for using readily transportable systems (i.e. laptops) for unclassified processing in the secure facility.

Enter Narrative Here

3.8.4 Hardware Acquisition

Describe the procedures for introducing hardware into the secure facility.

Enter Narrative Here

Web Protocol and Distributed/Collaborative Computing

3.9.1 Web Server Security

For Web protocol systems, describe the security of the servers.

Enter Narrative Here

3.9.2 Mobile Code

For Web protocol systems, describe the use of mobile code.

Enter Narrative Here

3.9.3 Executable Code

For Web protocol systems, describe how executable code is handled.

Enter Narrative Here

3.9.4 Collaborative Computing

If applicable, describe any collaborative computing process or applications.

Enter Narrative Here

3.9.5 Distributed Processing

If applicable, describe any distributed processing employed by the system.

Enter Narrative Here

4 BACKUP POLICY AND PROCEDURES

Describe the policy for backing up the system's information. This policy should reflect the system's designated Levels-of-Concern for Integrity and Availability. Provide detailed procedures for performing system backups.

Enter Narrative Here

5 RESTORATION POLICY AND PROCEDURES

Describe the policy for restoring information to the system. This policy should reflect the system's designated Level-of-Concern for Availability. Provide detailed procedures for restoring information to the system, to include a full system recovery.

Enter Narrative Here

6. KNOWN VULNERABILITIES AND RISK MITIGATION APPROACH

Describe known security vulnerabilities regarding the configuration and use of administrative functions.

Enter Narrative Here

Identify any risk mitigation approaches to alleviate identified vulnerabilities.

Enter Narrative Here

ADDITIONAL SECTIONS
Additional sections may be added as necessary to meet documentation requirements for the system's designated Protection Level and Levels-of-Concern for Integrity and Availability. These sections may include:

- Incident Response Plan
- Contingency Plans
- Trusted Recovery Procedures
- Maintenance Procedures

As an example,

Maintenance Procedures

Describe the procedures to be used for maintenance or repair of defective systems.

Enter Narrative Here

Describe the procedures for using lower or uncleared maintenance personnel.

Enter Narrative Here

Describe all system hardware maintenance logs, the information recorded on them, the individual responsible for reviewing them, and how often they are reviewed.

Enter Narrative Here